



Samsung KNOX Training Enterprise Troubleshooting

Enterprise Edition

Published: Oct 1, 2013
Version: 1.0



Course Objectives



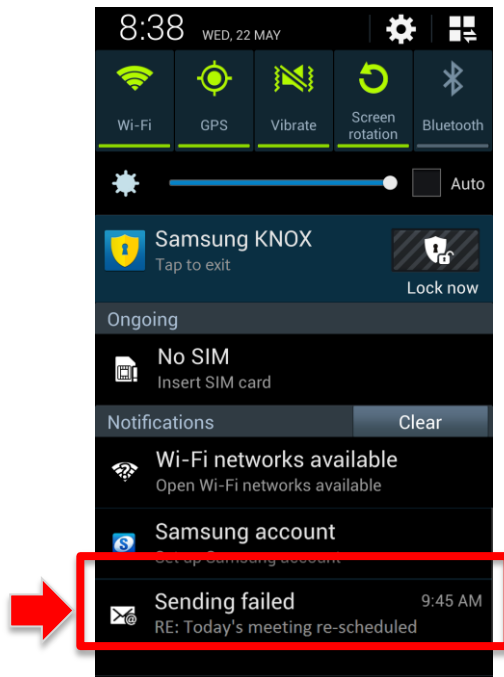
- Enable IT Administrators to understand:
 - KNOX troubleshooting features and tools.
 - KNOX device troubleshooting concepts and practices.
 - How to escalate issues to obtain advanced customer support .

Samsung Knox



Notifications Bar

Samsung Knox



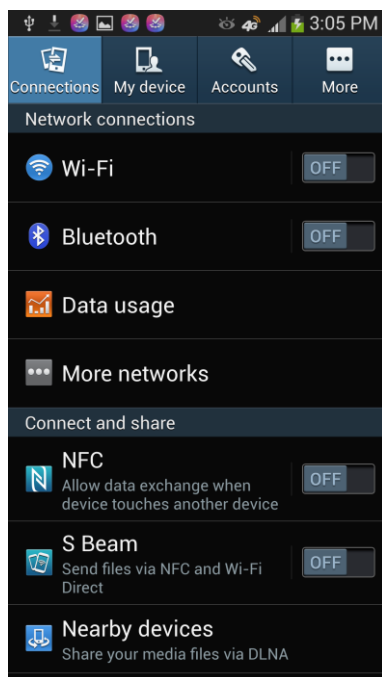
Use to check:

- Error notifications.
- Wi-Fi connectivity.
- KNOX Status notifications.

To display:

1. Swipe downwards from the top of the phone.

Settings



Use the *Settings* menu to perform the following:

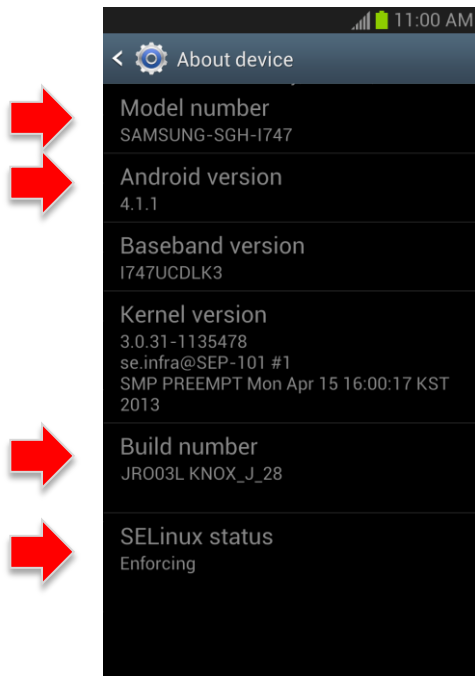
- Determine Version and Build Information.
- Edit and check KNOX Settings.
- Check Device Status.
- Check Wi-Fi Status.
- Check the Task Manager.
- Check App Info.

To display:

1. Access the *Settings* menu by

- Tapping the Settings icon on the desktop or by...
- Pressing and holding the Home button and selecting *Settings* from the Task Switcher menu, or...
- Pull down the Notifications view and tapping the Settings icon.

Version and Build Info



Use to check:

- Model number - Indicates the operator, e.g., I747/I337 is AT&T, 545 is Verizon (see the following slide).
- Android version - KNOX requires 4.1.1 on Galaxy SIII, 4.2.2 on Galaxy SIV.
- Build number - Indicates code family (J=Jellybean), branch (R=primary), date (O03=July 3, 2012), and build (L=#12).
- SELinux status - Before KNOX activation = Permissive, after = Enforcing.

To display:

Settings > More > About device.

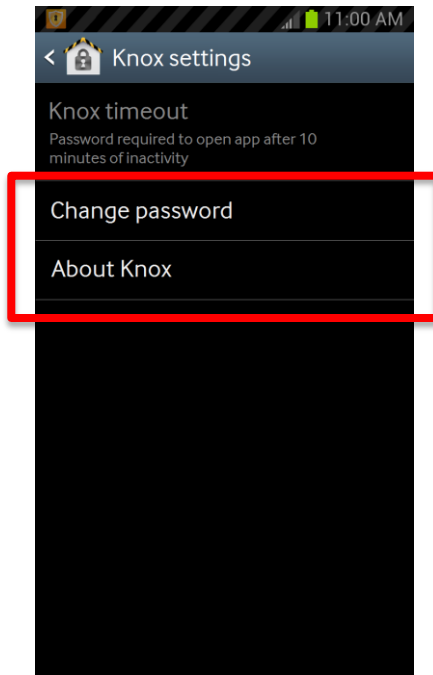
Device Model Number



The model number of the device indicates the carrier:

Carrier	Model #
AT&T, Bell	I337 (S4)
Open Europe	I9505 (S4)
Sprint	L720 (S4)
T-Mobile	M919 (S4)
US Cellular	R970 (S4)
Verizon	I545 (S4)

KNOX Settings



Use to:

- Change the password that the device user enters to switch to the business space. (Requires old password).
- Check the KNOX version installed.
- Display the End User License Agreement (EULA).

To display:

1. From within the Container view, tap the Menu key (lower left button) and select **KNOX settings**.
2. From this view you can change your password, determine your KNOX application version, or view the KNOX EULA.
3. Tapping **Change password** will navigate you to the password change screen.
4. Tapping **About KNOX** launches the Samsung KNOX *Application version* screen. Tap the Terms and Conditions button to view the EULA.

Device Status

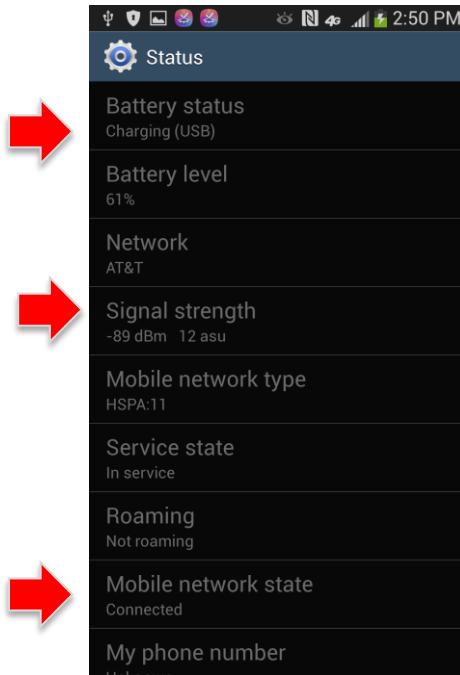


Use to:

- Check Battery level. If user-controlled KNOX device activation is enabled, battery level must be >70%.
- Check Signal strength. The KNOX activation process requires a stable cellular or Wi-Fi connection.
- Check Mobile network state. If downloading files over cellular, the status must be "Connected".

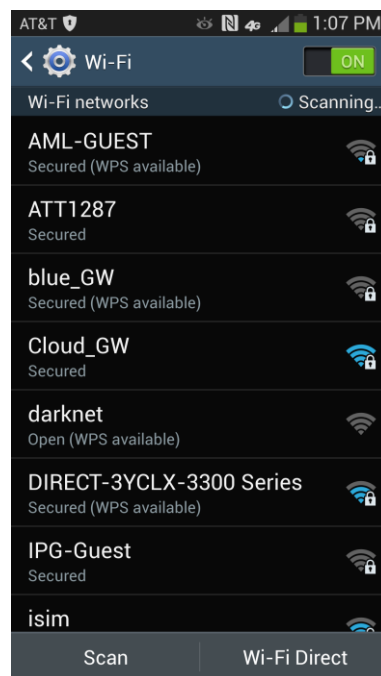
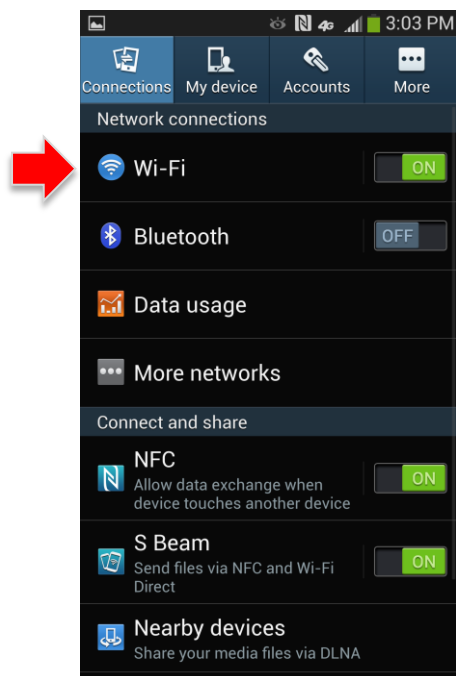
To display:

1. ***Settings > More > About device > Status.***



Wi-Fi Status

Samsung Knox



Use to:

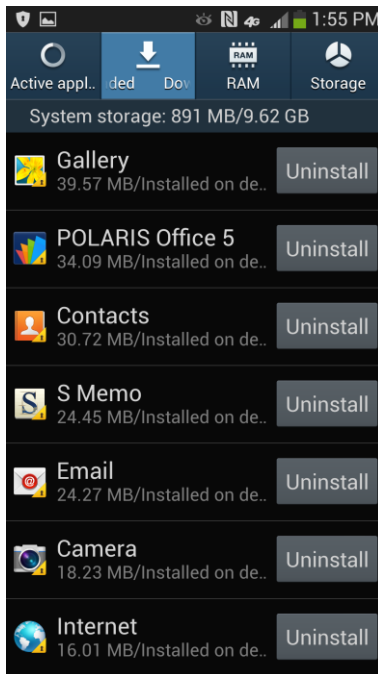
- Check Wi-Fi connectivity and signal strength. Some file downloads may be allowed over Wi-Fi only. For example, the update package downloaded during the initial KNOX activation, may be enabled by the MDM app on the device for Wi-Fi.

To display:

1. Tap **Settings** to display the *Connections* view.
2. Tap **Settings** > **Wi-Fi** to view available *Wi-Fi networks* and to view signal strength.

Task Manager


Samsung Knox



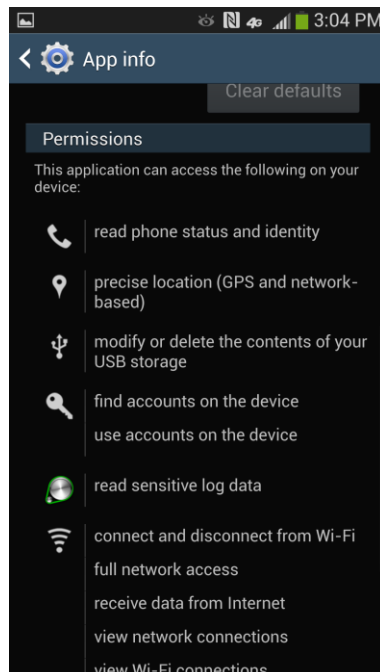
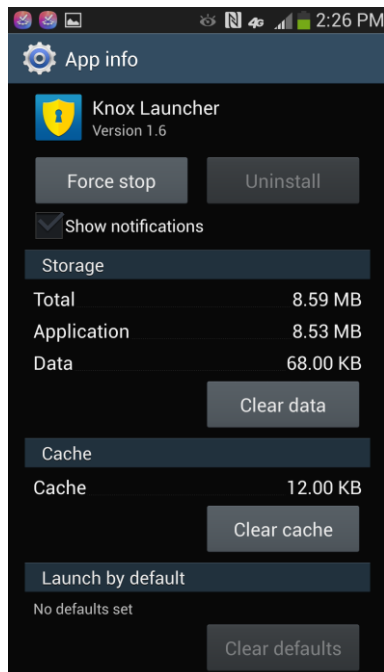
Use to:

- Check (and end) running apps.
- Check (and uninstall) downloaded apps.
- Check memory usage.
- Check available disk space.

To display:

1. Push and hold **Home** button.
2. Tap the **Task Manager** icon 
3. Select either *Active applications* or *Downloaded applications* buttons.
4. Tap the *RAM* or *Storage* icons to provide indication of system resources being consumed.
5. Tap the individual app to display App Info.

App Info



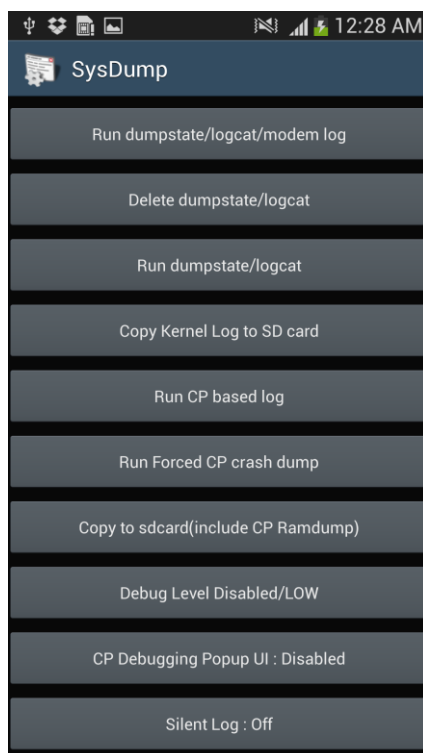
Use to:

- Check an app version number.
- Stop or uninstall the app.
- Check the app's disk space or memory usage.
- Clear data or cache.
- Check granted permissions, e.g., access to network, location, phone, hardware control .

To display:

1. Tap **Settings > More > Application Manager**.
2. Navigate to the **All** view.
3. Tap the **App name** to view App Info.
4. Scroll down to view App **Permissions** info.

SysDump Log Capture



There are times where Samsung Support or MDM representative may ask the IT admin to send log file information so they may determine the cause of a particular device behavior issue. In those cases, the IT Admin should use the SysDump tool to get logs from device.

To get logs using SysDump:

1. Call ***#9900#**.
2. Tap **Run dumpstate/logcat**.
Saves logs to internal storage:
/data/log/dumpState_yyyymmddn.log
3. Tap **Copy to sdcard**.
4. Launch **My Files**.
5. Go to **/log** folder.
6. Share the log file with Samsung Support via email, Wi-Fi, Bluetooth, USB, Dropbox, etc.

Additional Resources



Samsung Galaxy:

- [Samsung Galaxy S4 User Manual](#)
- [Manuals and Troubleshooting Guide](#)

Samsung KNOX :

- [Samsung KNOX White Paper](#)
- [Samsung KNOX Support Portal](#)

Samsung Galaxy & KNOX interactive Flash simulations:

- [AT&T Galaxy SIV](#)
- [Verizon Galaxy SIV](#)

Operator resources:

- AT&T – [Device How-to](#), [Troubleshoot Your Device](#)
- [Verizon](#) – Videos, Device Questions, Articles

Cannot Activate KNOX



To activate KNOX, an update package must be downloaded to the device from a Samsung update server. The server may be not be accessible, the device may not be adequately charged, or the server may be down or unable to respond to package requests within a specified timeout period.

1. Verify the device battery charge level is greater than 70%. If not, have the user plug the device into a charger and reattempt the activation.
2. If the battery level is OK, verify that Wi-Fi is On, with good Wi-Fi signal strength (if using Wi-Fi connection).
3. If the user is using a cellular connection, check that Mobile Data is **On**, with good cellular signal strength (if using a cellular connection).
4. In case this is a due to a sporadic event, like abnormally high network traffic or unplanned server maintenance, check with IT or try the device activation again at a later time.
5. If unsuccessful, escalate the issue.

Samsung Knox



“Device Activation has Failed” Message

KNOX activation was performed on a device, the update package was downloaded, and the device rebooted, but the device displays a message indicating that activation failed. There may be an issue with the update package.

1. Escalate this issue through the MDM vendor.
2. Postpone activating any additional devices until you get further instructions.

Cannot Create a Password



IT can set strict requirements for the container password, e.g., set up forbidden strings, restrict the re-use of past passwords, check password strength, restrict the use of characters.

1. Use the MDM console, check the KNOX container password policies and verify the user's password complies with these policies.
2. If the **Show password** option is available, ensure that both passwords match, and case sensitivity is not an issue.
3. If the issue remains, remove and re-create the container on the user's device.
4. If symptoms persist, escalate the issue.

Locked Out of KNOX Container



The user has failed to enter the correct KNOX password and may have exceeded the allowed number of tries. This number can be set by IT Admins through the MDM console.

1. Reset the user's Container password using the attending MCM/MDM system.
2. Ask the user to create a new password.

KNOX Startup and Login



- After KNOX has been activated, it takes a couple of minutes to start up:
 - Create the container.
 - Set up a secure file system.
 - Install the required components.
 - Pre-load apps.
- A progress bar with messages indicates the status. On successful creation, the user launches KNOX and enters their password and to visit the business space.
- Any time there is inactivity in the business space (by default, for 10 minutes), the user must re-enter their password.

Cannot Log into KNOX



The user may be using the wrong password or may have recently changed their KNOX password.

1. Ask user to verify and re-enter their KNOX password. If this doesn't work, proceed to the next step.
2. Reset the user's Container password using the attending MCM/MDM system.
3. If symptom persist, remove and re-create the container on the user's device.
4. If symptoms persist, escalate the issue.

Business Email not Synced



There may be a problem with device reception, NT login, ActiveSync, Active Directory issues, or issues with the enterprise Exchange server.

1. Check the following:

- Device has cellular/Wi-Fi connectivity.
- Verify the user has not changed their NT password recently. If so, have them update the password in the device (note that some carriers send a notification instructing the user to update their password).
- Reboot the user' device.
- Also check that....
 - o Domain, user login, and password are correct (ActiveSync is working and sync settings have not changed).
 - o Active Directory is working and account is not locked or in a bad state.
 - o Exchange server access state is OK and not Denied.

2. Remove and re-create the email account.

3. If symptoms persist, escalate the issue.

Cannot Download from App Store



User cannot download from the KNOX App Store.

1. Try the following:
 - Check that device has network connectivity.
 - Check that user is logged in.
 - Restart the app download.
 - Restart the device.
 - Clear the cache used by App Store, download manager.
2. Try downloading using another KNOX device, to determine whether the issue is with one device only.
3. If this fails, escalate the issue.

No VPN Connection



An app that uses VPN is not able to access Internet, e.g., container-based browser cannot display web pages.

1. Check the underlying network connection:
 - Wi-Fi is On, with good Wi-Fi signal strength.
 - Cellular access is up, Mobile data is On.
2. Perform a device reboot. If symptoms persist...
3. Check if the VPN connection has ever worked. If it never has:
 - Using another device, test the app and VPN connection.
 - At the MDM console, check the VPN profile, policy settings.
 - Ensure that the VPN gateway is operational.

VPN Connection Not Stable



An app that uses VPN to access to the Internet works sporadically. Due to user roaming, the device may be switching between Wi-Fi and cellular networks.

1. Check the underlying network connection:
 - Wi-Fi is On, with good Wi-Fi signal strength.
 - Cellular access is up, with good signal strength.
 - Device is not roaming when testing connection.
2. Check if the VPN server went down momentarily.
3. If symptoms persist, escalate the issue.

VPN Access Point Times Out



The VPN goes through an access point (like a Wi-Fi router at home) which has not been configured to enable VPN.

1. Check the access point firewall settings.
 - VPN requires UDP ports 500 and 4500 to communicate.
 - Enable VPN passthrough.
2. If symptoms persist, escalate the issue.

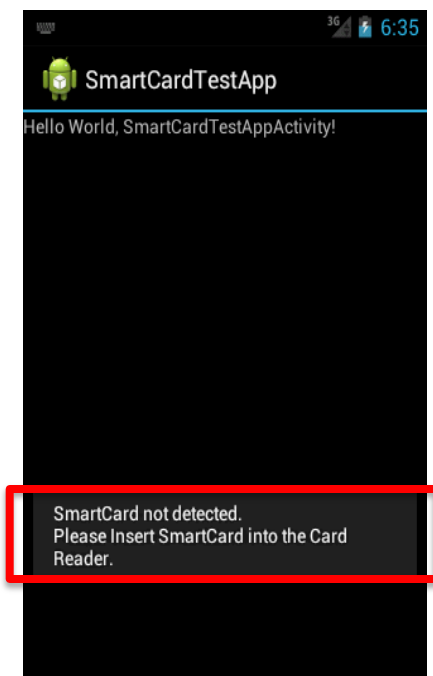
VPN Observed Timeout/Host Not Found



VPN Observed Timeout/Host not found

1. Ensure that you have good signal strength if you using a data connection.
2. Ensure that there is no firewall policy preventing access.
3. Verify there are no Wi-Fi Access Point restrictions imposed.
4. If symptoms persist, escalate the issue

CAC Issues (DoD)



- Generally for errors, a toast will be shown that provides minimum interruption to the user. For a connection error, a sample toast message is shown.
- The following are CAC error messages and associated actions:
 - **CAC Card Removed** – insert/reseat card in the reader.
 - **CAC PIN Error** – verify and re-enter the PIN.
 - **CAC PIN Expired** – re-enter PIN due to timeout.
 - **Uninitialized CAC Card** – contact the CAC administrator.
 - **CAC Locked** (after three incorrect login attempts) – see the next page for user guidance.
 - **No Connection** - Connection to the Smart Card does not exist possibly due to card not present in reader or reader is out of range.
 - **Device Not Configured** - Indicates that the Smart Card Reader is not configured on the device. Possibly device is not paired.
 - **Connection Busy** - Indicates that the connection is already established.

CAC PIN is Locked (DoD)



DoD personnel using a CAC can encounter a Personal Identification Number (PIN) on the CAC that is locked. Usually this takes place after three unsuccessful login attempts. You must contact an appropriate DoD facility to reset the CAC PIN.

To unlock a CAC:

1. Contact any DEERS/RAPIDS issuing facility and they can reset a CAC PIN. Please locate your nearest DEERS/RAPIDS ID Card facility using the RAPIDS Site Locator. The web address follows:

<http://www.dmdc.osd.mil/rsl/>

Additional CAC and CAC reader information:

<http://www.cac.mil/>

[BAI M3000 Android Bluetooth Reader Users Guide](#)

Error Notifications



The following describes the prevention and detection error notifications for SE for Android and TIMA errors.

Mode	Component	Reason	Notification Detail
Prevention	SE for Android	Policy denial	The application is forced to stop due to unauthorized behavior of the software. This may be caused by: <ul style="list-style-type: none"> Unauthorized attempt to access information in your device
	TIMA	LKM detection	The system kernel is forced to stop loading an unrecognized kernel module. The unrecognized module may contain malicious code and compromise the system. This may be caused by: <ul style="list-style-type: none"> Unauthorized attempt to load malicious code into the kernel of your device
Detection	TIMA	SE for Android mode change	SE for Android has been disabled on your device. This may lead to further security compromises. This may be caused by: <ul style="list-style-type: none"> Unauthorized attempt to compromise the kernel of your device. Accidental disabling of SE for Android enforcement on your device.
	TIMA	Periodic measurement	There has been unauthorized modification to the kernel on the device. This may allow malware to completely take over the device. This may be caused by: <ul style="list-style-type: none"> Unauthorized attempt to inject code into the kernel of your device. Unauthorized installation of malicious kernel modules on your device.

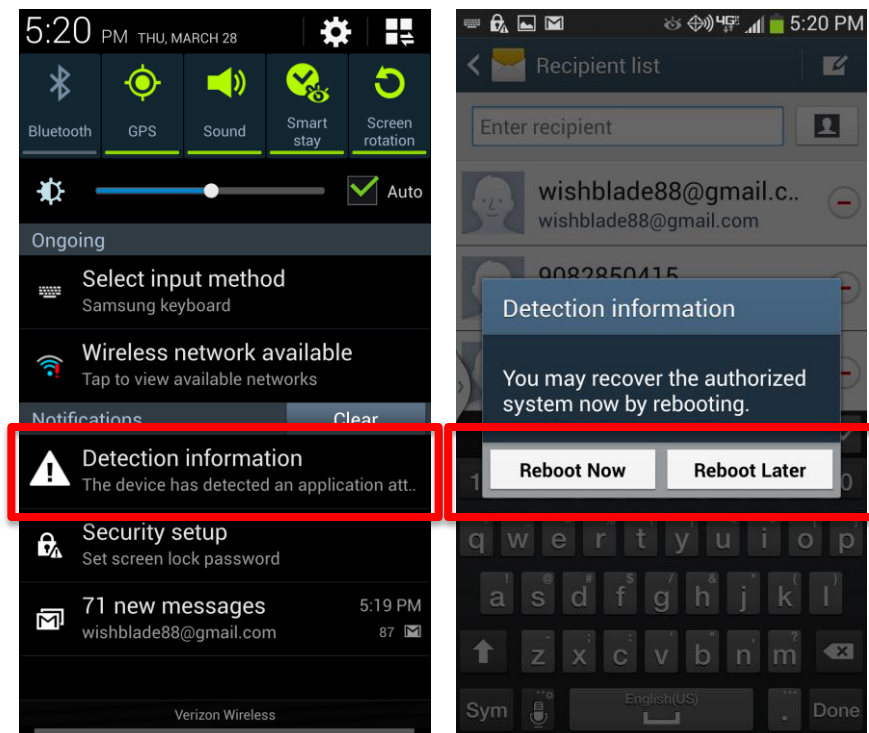
Denial Log



When an SE for Android™ policy violation is detected, policy denial information is uploaded to the KNOX denial server for analysis. The denial log does not contain any personal information such as the IMEI.

Activity	When Triggered	Remarks
Denial Log	<p>When a third party application attempts to access (read/write) an unauthorized system resource.</p> <p>The unauthorized access is denied and information is saved to the denial log.</p>	<p>Log date</p> <ul style="list-style-type: none"> • Timestamp, detail of access ({}) • Access module PID • Denied access command • Source context of the access (scontext, source context) • Target context of the access (tcontext, target context) • Class type of the access module (tclass) <p>Example</p> <ul style="list-style-type: none"> • Audit(1356998688.587:167):avc: denied { read } for pid=7749 comm="dumpstate" name="exe" dev="proc" ino=31205 scontext=u:r:system_pp:s0 <p>Location of log on device</p> <ul style="list-style-type: none"> • /data/misc/audit/audit.log/
Server Upload	<p>Configurable log upload period.</p> <p>The default is weekly.</p>	<p>Transfer Detail</p> <ul style="list-style-type: none"> • Transfer protocol: https (secure protocol) • Transfer file format: compressed file (gzip)

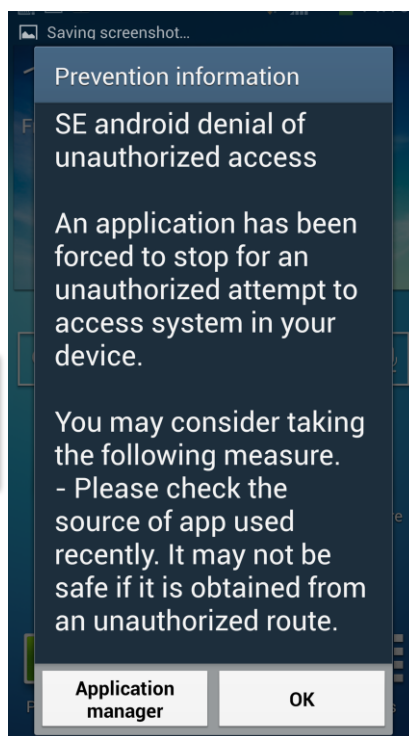
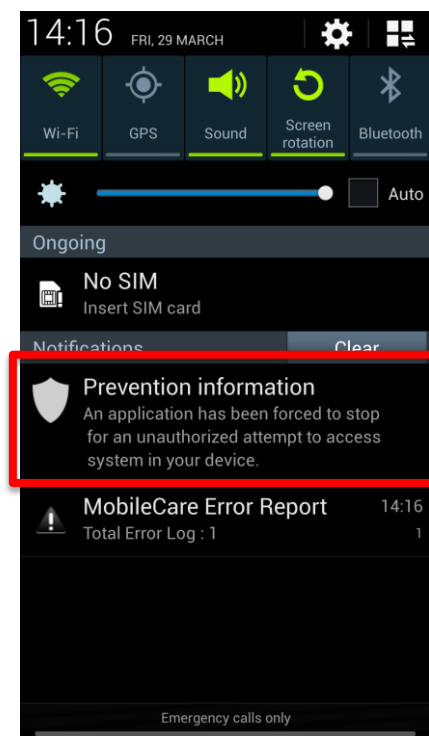
"System has been Compromised" Message Samsung Knox



The device displays one of these messages for TIMA-related events:

- *The device has detected an application attempting unpermitted actions and has stopped loading. To protect your device, it is recommended you reboot.*
 - *The device has detected an application attempting unpermitted actions. To protect your device, it is recommended you reboot.*
 - *SE for Android protection has been disabled. To protect your device, it is recommended you reboot.*
1. Attempt reboot of the device.
 2. If symptoms persist, escalate the issue.

SE for Android Denial



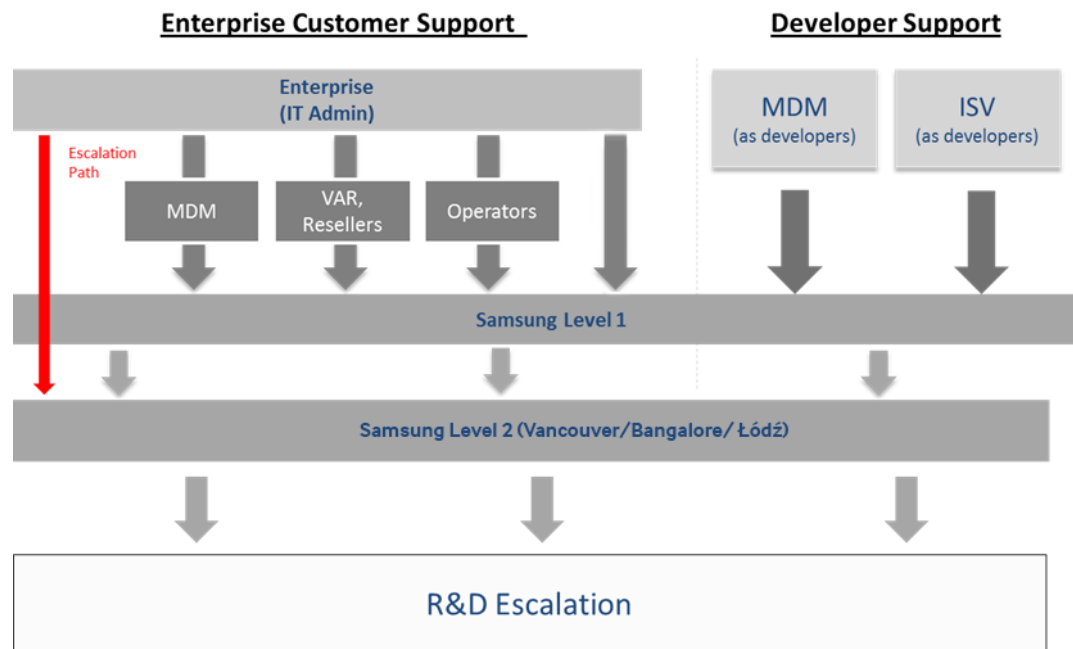
SE for Android denial events occur when there is an unauthorized attempt by an app to access the system.

- An alert will appear in Notifications (filtered text) and a popup will display in the KNOX Container giving the option of:
 - Navigating to the Application manager.
 - Dismissing the Alert window.
1. Tap “OK” to dismiss the error window.
 2. If symptoms persist, attempt a reboot of the device.
 3. If symptoms continue to persist, escalate the issue.

Samsung Knox



Samsung KNOX Support Model



- You can use any of the following channels to escalate an issue:
 - Web form on the KNOX Support Portal at www.support.samsungknox.com
 - By Phone at 1-855-567-KNOX

Submitting an Issue



New ticket [▼ apply macro](#)

Requester
Start typing and we'll look up matching users.

CC
Start typing and we'll look up matching users.

Subject

Status Type Group Assignee* Subject Category* [▼ \[no selection\]](#)

Priority Severity* ☐ Confirm customer-defined priority severity*

☐ Fix required. No possible workaround. Ticket Reference Number (from Solution/Channel Partners)


PLM id Redmine id Knox version*

Model number Device IMEI Device Build number

Device Kernel version Network carrier Connection type ☐ Roaming

Mobile Network State

Customer (Company) MDM

Description (required) 

[Attach file >](#)

Create ticket (ctrl-s)

To complete the Web Form:

1. Go to www.support.samsungknox.com
2. Click **Submit a Request**.
3. Fill out the request form (see the next slide for instructions).
4. Click **Submit**.

Describing the Issue



- Please prepare the following information when contacting Samsung Support through phone and web form:
 - **Description:** Include any information that is not already in the fields above. For example:
 - **Location:** Indicate the region where the issue is occurring.
 - **Device model number and Android version:** Settings > About Device > Model Number/Android Version
 - **Device Build number:** Settings > About Device > Build Number
 - **Device Kernel version:** Settings > About Device > Kernel Version
 - **Network carrier and type**
 - **Device IMEI:** Settings > About Device > Status > IMEI
 - **Connection Type:** The type of connection the device is using to connect to the enterprise network.
 - **Mobile Network State:** Indicate whether the issue is occurring while the device is connected to a mobile network.

Escalation Severity and Priority



Severity/Priority	Description	Examples
1	Services or applications provided by Solution and Channel Partners or Samsung are inoperative or there is a security breach. The incident is affecting a significant number of users and severely impacting normal business operations. No solution is immediately available.	<p>Critical applications within the container, such as Email, are not functioning for a significant numbers of users across the organization.</p> <p>A security breach has occurred which could result in an unauthorized third-party gaining access to the organization's data.</p> <p>Normal operation of the organization is severely impacted.</p>
2	There is widespread impairment of portions of the services or applications provided by Solution and Channel Partners Samsung. The incident is affecting a significant number of users and impacting normal business operations. No solution is immediately available.	Critical applications within the container, such as Email, can be used sporadically. For instance, some users can receive, but not send emails. Normal operation of the organization is impacted
3	Portions of the services or applications provided by the solution partner or Samsung are impaired. The incident is affecting a small number of users and minimally impacting normal business operations.	Critical applications within the container, such as Email, are not operating with full functionality. For instance, users cannot open attachments with the Email app. Normal operation of the organization is minimally impacted.
4	There is a minor impairment of portions of the services or applications provided by the solution partner or Samsung. The incident has little or no impact on users and normal business operations.	The Enterprise IT administrator is trying to push an update of the Email app to users and requires further instructions. There is little or no impact on the normal operation of the organization.



Thank you for supporting
Samsung KNOX.

© 2013 Samsung. Samsung, Galaxy S, SAFE, and Samsung KNOX are all trademarks of Samsung Electronics Co., Ltd. Android and other marks are trademarks of Google Inc. Other company and product names mentioned herein may be trademarks of their respective owners.

All functionality, features, specifications, and other product information provided in this document including, but not limited to, the benefits, design, pricing, components, performance, availability, and capabilities of the product are subject to change without notice or obligation. Samsung reserves the right to make changes to this document and the product described herein, at anytime, without obligation on Samsung to provide notification of such change.